California Public Employees' Retirement System

Attachment 1

Information Security Office
Information Security Internal Incident Tracking Log

Official (Via E-Mail) Notification Date of Incident Sent to ISOF	Originating Division or Office	Working Title	Type of Incident	Comments
8/30/2010	CalPERS CSED Employee	Unauthorized my|calper	Unauthorized my/CalPERS account creation	A member called to report that an unauthorized my/CalPERS account was created. An investigation revealed that the account was successfully created by answering two security questions (i.e., the correct mailing address and the correct current employer). A letter was mailed to the member outlining the details of the date, time, and IP address used to create the account.
9/2/2010	CSED	Unauthorized Disclosure of Social Security Number	Unauthorized Disclosure of Personally Identifiable Information	This incident involved the unauthorized disclosure of the Social Security number for one CalPERS Member, to another CalPERS Member. The incident occurred when one member received a requested direct deposit form. Included in the packet were letters for several other members, including the Benefit Approval Letter for the second CalPERS Member. Based on the investigative work performed to date (11/4/10), the ISOF infers on the basis of the evidence collected and examined that the Social Security number for the second CalPERS member was disclosed to member requesting the direct deposit form in an unauthorized manner. A Privacy Breach Notification letter is not necessary pursuant to California Civil Code Section 1798.29 because the breach was not automated. A letter offering CSIdentity Theft Insurance was mailed to the member.
9/7/2010	INVO	Sharing UserIDs	Violation of CalPERS Policy	Based on the investigative work performed to date (09-08-10), the ISOF infers on the basis of the evidence collected and examined that an Investment Officer II, INVO, accessed the computer assigned to an AGPA, in the CalPERS Investment Office. Although there was no indication of mal intent this access action violated the CalPERS Information Security *Identity Authentication Practice* which states: "*UserIDs are to be used only by the person to whom they are assigned. User IDS are unique and may not be assigned to more than one person.*" At the request of the Division Chief, INVO, both employees will be retaking the CalPERS *Information Security Awareness* Web-Based Course.
9/7/2010	CalPERS SMSD Employee	900 Telephone Scam	Possible Disclosure of Member Information	A CalPERS member contacted SMSD to notify us of a possible problem with our Call Center number. When the member called she received a message redirecting her to a 900 number. Based on the investigative work performed to date (09-09-10), the ISOF infers on the basis of the evidence collected and examined that the member misdialed the CalPERS Call Center at (888) 225-7377 and was redirected. to a 900 scam number. We have not been able to recreate the problem.
9/29/2010	ITSB	Missing Blackberry	Missing Blackberry	Based on the investigative work performed to date (10-01-10), the ISOF infers on the basis of the evidence collected and examined that Information Technology Services Branch employee, first noted his CalPERS assigned BlackBerry 9700 Bold smartphone handheld device was missing at about 10:00 a.m. on Wednesday, September 29, 2010. He states that no sensitive data was stored on the smartphone. The device was disabled.
10/7/2010	Board Member	Missing Blackberry	Missing Blackberry	Based on the investigative work performed to date (10-14-10), the ISOF infers on the basis of the evidence collected and examined that the Board Member, first noted his CalPERS assigned BlackBerry Bold 9700 smartphone handheld device was missing at about 9:00 a.m. on Tuesday, October 5, 2010. He states that no sensitive data was stored on the smartphone. The device was disabled.

California Public Employees' Retirement System

Information Security Office
Information Security Internal Incident Tracking Log

Official (Via E-Mail) Notification Date of Incident Sent to ISOF	Originating Division or Office	Working Title	Type of Incident	Comments
10/13/2010	HBB	Anthem Blue Cross - Blue Sheild CD ePHI	HIPAA Security	CalPERS staff received an e-mail message from the Enrollment and Billing Representative, at Anthem Blue Cross, on August 18, 2010 informing CalPERS that the CD received for the May 2010 reconciliation period contained ePHI for Blue Shield members instead of for Anthem Blue Cross members. The specific ePHI disclosed were Social Security numbers, health plan names, and health premium rates. Prime life subscribers through Blue Shield (Access +, NetValue, Advantage, and NetValue Advantage) ePHI was also disclosed. Anthem Blue Cross accidentally received Blue Shield reconciliation data. The Enrollment and Billing Representative confirmed that the data received was not further used or disclosed by Anthem Blue Cross. The CD was returned to CalPERS via UPS Overnight from Anthem Blue Cross on September 8, 2010. Staff retrieved the information from the mailroom and the CD was destroyed via shredding the same day. This Security Internal Event is not considered a breach under HIPAA because of the exclusion at 45 CFR Part 164.402 Breach (2)(ii). The information was not disclosed to an uncovered enitity.
10/18/2010	ITSB	Virus Activity (Trojan)	Security Compromise	A PSR computer located in Accenture's Development Network (ADE) was presumably infected with malware. It appears that on 10/01/2010 the Accenture PC was responsible for placing 3 malicious files and 1 directory on a CalPERS Drive. For security reasons the information on the files is not being included in this report. Desktop support noticed malicious activity and notified their management on 10/15/2010. On 10/18/2010 the Security Administration Section (SAS) was notified. SAS found 3 instances in the enterprise where the malicious exe was detected on local computers. This *file* was successfully removed by McAfee. SAS considers this malware contained. McAfee is the standard virus scan running on CalPERS workstations. Detecting this variant on the desktop prevented any outbreak. Lessons learned will be shared internally.
10/21/2010	EXEO	Lost RSA Token	Lost RSA Token	Based on the investigative work performed to date (10-26-10), the ISOF infers on the basis of the evidence collected and examined that the CalPERS Executive Office employee misplaced her assigned RSA token on either October 19 or October 20, 2010. The misplaced token was disabled and noted as lost.
10/26/2010	FCSD	Missing Blackberry	Missing Blackberry	Based on the investigative work performed to date (11-05-10), the ISOF infers on the basis of the evidence collected and examined that the Fiscal Services Division employee, first noted her CalPERS assigned BlackBerry Bold 9700 smartphone handheld device was missing on Monday, October 25, 2010. She states that no sensitive data was stored on the smartphone.The device was disabled.
10/27/2010	ITSB	Lost RSA Token	Lost RSA Token	Based on the investigative work performed to date (10-28-10), the ISOF infers on the basis of the evidence collected and examined that the Information Technology Services Branch employee misplaced his assigned RSA token prior to Tuesday, September 7, 2010. The misplaced token was disabled and noted as lost.
11/12/2010	INVO	Missing Blackberry	Missing Blackberry	Based on the investigative work performed to date (11-16-10), the ISOF infers on the basis of the evidence collected and examined that the Investment Office employee first noted his CalPERS assigned BlackBerry Bold 9700 smartphone handheld device was missing on November 4, 2010. He states that no sensitive data was stored on the smartphone. The device was disabled.
11/15/2010	OSSD	Unauthorized Disclosure of Social Security Number	Unauthorized Disclosure of Personally Identifiable Information	Based on the investigative work performed to date (11-18-10), the ISOF infers on the basis of the evidence collected and examined that the Social Security number for one CalPERS Member, was disclosed to another CalPERS Member, in an unauthorized manner. A Privacy Breach Notification letter is not necessary pursuant to California Civil Code Section 1798.29 because the breach was not automated. A letter offering CSIdentity Theft Insurance was mailed to to the member.